Wisconsin Service**Point**

ROLES AND RESPONSIBILITIES:

Policy:
The HMIS, vendors, staff and agency partners will maintain and monitor database integrity.

Standard:
Definition of roles for HMIS.

Purpose:
To outline the major responsibilities of the HMIS Vendors, Staff and Users.

Supporting Documents

Resources:

HMIS WEB SITE (WISP)
https://wisconsin.servicept.com

HMIS INFOrmed
www.hmis.info/default.asp

Wisconsin HMIS
http://wisp.wi.gov

WISP HELP
sphelp@commerce.state.wi.us

RESPONSIBILITIES OF HMIS ROLES

Steering Committee
a. Taking responsibility for the implementation and continuous improvement of the HMIS.
b. Ensuring the HMIS scope aligns with the requirements of agencies, HUD and other stakeholder groups.
c. Addressing any issue that has major implications for the HMIS be it policy mandates from HUD or performance problems with the HMIS vendor.
d. Reconciling differences in opinions and approaches, and resolving disputes arising from them;
e. Approving policy for users of the HMIS.

Software Vendor (*Bowman Systems*)
a. Designing the application to meet National HUD Data Standards.
b. Developing a codebook and other documentation of programs created.
c. Providing ongoing support to HMIS System Administrators pertaining to the system.
d. Providing ongoing support to the HMIS System Administrators pertaining to needs of end-users to mine the database, generate reports and other end-user interface needs.
e. Administration of product servers including web and database.
f. Monitoring access to these systems through auditing.
g. Monitoring functionality, speed and database backup procedures.
h. Backup and recovery of internal and external networks.
i. Operating the system web site twenty-four hours a day, seven days a week.
j. Communicating any planned or unplanned interruption of service to the Human Service

System Administrators (*State of Wisconsin, Department of Commerce*)
a. Oversight of all contractual agreements with funders, participating organizations and consultants in adherence with the policies and practices of HMIS, and recommendations of the HMIS Steering Committee.
b. Monitoring compliance and periodically reviewing control decisions.

c. Communicating with participating organization leadership and other stakeholders regarding the HMIS project.
d. Authorizing usage and access to the HMIS.
e. Only authorizing users who need access to the system for technical administration, data entry, editing of client records, viewing of client records, report writing, administration of other essential activity associated with carrying out HMIS responsibilities.
f. Developing reports to present the data.
g. Mining the database to respond to the information needs of participating organizations, community stakeholders and consumers.
h. Documenting work on the database and in development of reports/queries.
i. Providing technical assistance as needed with program sites.
j. Providing training and technical assistance to participating organizations on policies and procedures, system use, authorizing access to the system including set-up, in response to questions from users, and in response to network and system functionality questions.
k. Coordinating technical support for system software.
l. Communicating with participants regarding problems with data entry and to support data quality.
m. Monitoring agency participation including timeliness and completeness of entry.
n. Communicating any planned or unplanned interruption in service.
o. Auditing policy and procedure compliance.

Provider Group Administrator (PGA)
a. Assessing HMIS capacity and making recommendations to each agency on how to improve their technology as it relates to the HMIS.
b. *A*ssessing current reporting needs and developing plans for improved and increased performance for programs currently entering data into HMIS and for the expansion of HMIS to programs that currently are not tracking their data in HMIS.
c. Representing HMIS in meetings to keep executive directors of partner agencies aware of what is happening both locally, state-wide and nationally on issues within HMIS that might affect their agency.
d. Either coordinating HMIS trainings that are available either at the Department of Commerce or that are hosted locally.
e. Communicating with participants regarding problems with data entry and supporting data quality.
f. Convening meetings of all the users within the PGA community to discuss issues related to HMIS and the direction that the local community is taking in regard to sharing data and recording services.
g. Reporting on aggregate data within the partner agencies.

Agency Administrator

a. Editing and updating agency information
b. Establishing which standard report is to be run for each specific program created.
c. Ensuring a minimum standard of data quality by answering all the HUD Universal Data Elements for every individual entered into the HMIS for the agency's programs.
d. Granting technical access to the software system for persons authorized by creating usernames and passwords;
e. Training new staff persons on the uses of the Service Point software system including review of the policies and procedures and any agency policies which impact the security and integrity of client information.
f. Ensuring that access to the Service Point system is granted to authorized staff members only after they have received training.
g. Notifying all users in their agency of interruptions in service.
h. Providing a single point of communication between end-users and HMIS staff at the Department of Commerce.
i. Administering data security policy and standards, including:
   - ✓ Administering and monitoring access control
   - ✓ Providing assistance in the backup and recovery of data
   - ✓ Detecting and responding to violations of the policies and procedures or agency procedures.

Users:

a. Taking appropriate measures to prevent unauthorized disclosure.
b. Reporting security violations.
c. Complying with relevant policies and procedures.
d. Inputting required data fields in a current and timely manner.
e. Informing clients about the agency's use of HMIS.
f. Taking responsibility for any actions undertaken with their usernames and passwords.